

了解ISE 3.3补丁4上AD的按需资源预留

目录

[简介](#)

[前提条件](#)

[所需组件](#)

[背景信息](#)

[症状](#)

[问题](#)

[解决方案](#)

[逐步配置](#)

[其他详细信息](#)

[故障排除](#)

[确认](#)

[日志记录](#)

[日志片段](#)

[常见问题](#)

简介

本文档介绍有关ISE 3.3补丁4上Active Directory的按需资源预留

前提条件

思科身份服务引擎(ISE)知识

Active Directory(AD)知识

有关ISE和AD集成的知识

所需组件

本文档中的信息基于以下软件和硬件版本

- 思科身份服务引擎3.3补丁4
- Microsoft Windows Active Directory 2016或最新版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

AD身份验证有时很慢，最终会失败。可能的原因可能是ADID队列开始堆积或所有ADID池线程耗尽。

有关ADID的更多详细信息：

ADID(也称为可分辨名称(DN))是一个字符串，用于唯一标识Active Directory目录中的对象。它们用于定位和管理Active Directory域中的对象。ADID对于管理Active Directory环境中的用户帐户、权限和其他资源至关重要。

典型的ADID必须如下所示：CN=John Doe，OU=Sales，DC=example，DC=com;其中，

CN=John Doe:表示用户的公用名John Doe。
OU=销售：表示用户所属的组织单位(OU)，在本例中为销售部门。
DC=example，DC=com:表示域组件，即example.com。

例如:

请参阅图1:典型的AD加入点配置

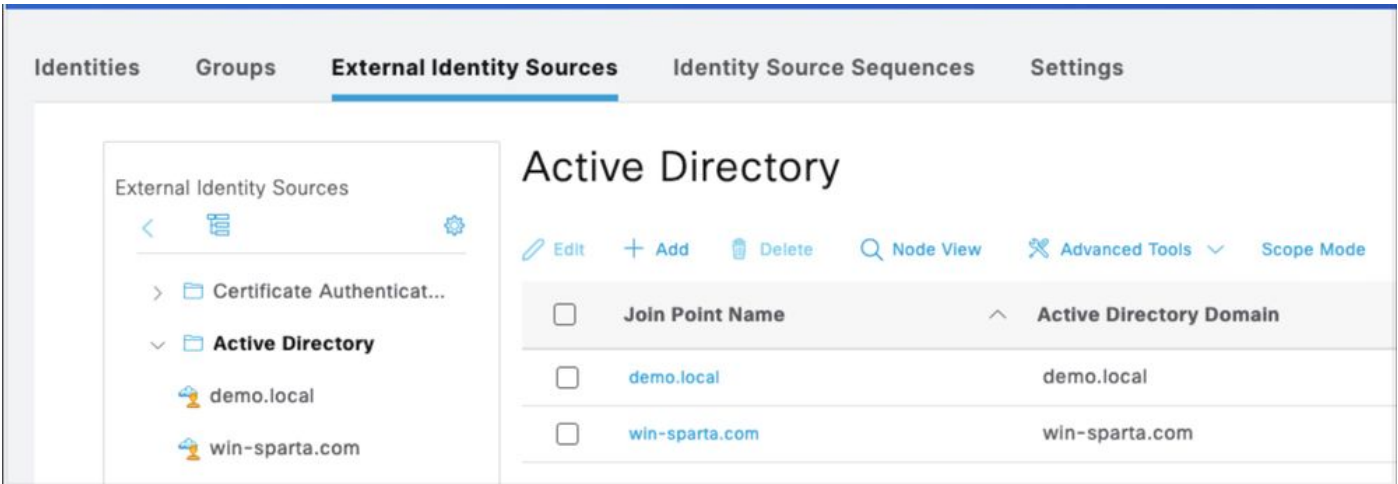


图 1：AD加入点

请参阅图2:具有2个连接点的典型AD流程图

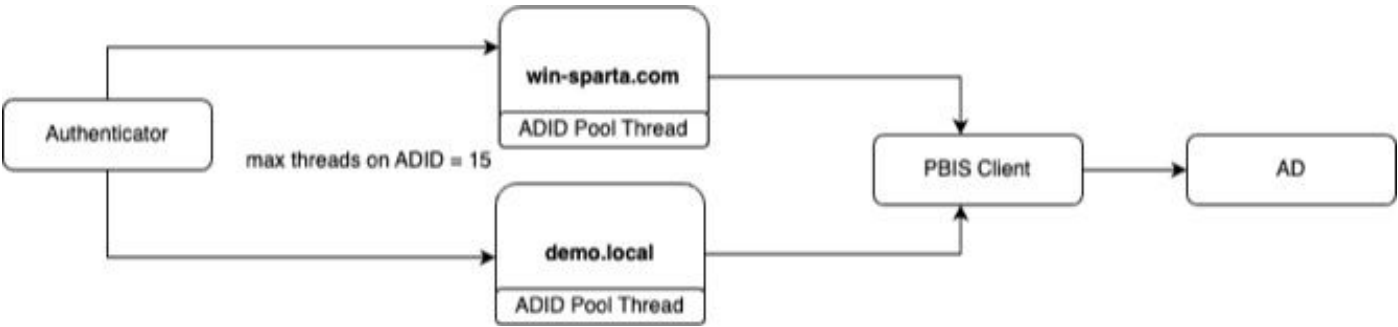


图 2：典型的AD流程图

症状

同一ADID线程池下的慢加入点

问题

1. 其中一个加入点速度非常慢的后果是什么？例如，如果“demo.local”和“demo.local”的15个身份验证同时发送到ISE的速度异常缓慢，我们需要等待“demo.local”的响应，然后再处理后续的win-sparta身份验证。
2. 如果两个加入点在一个加入点下共享同一个ADID线程池会怎样？

请参阅图3:慢节点流程图

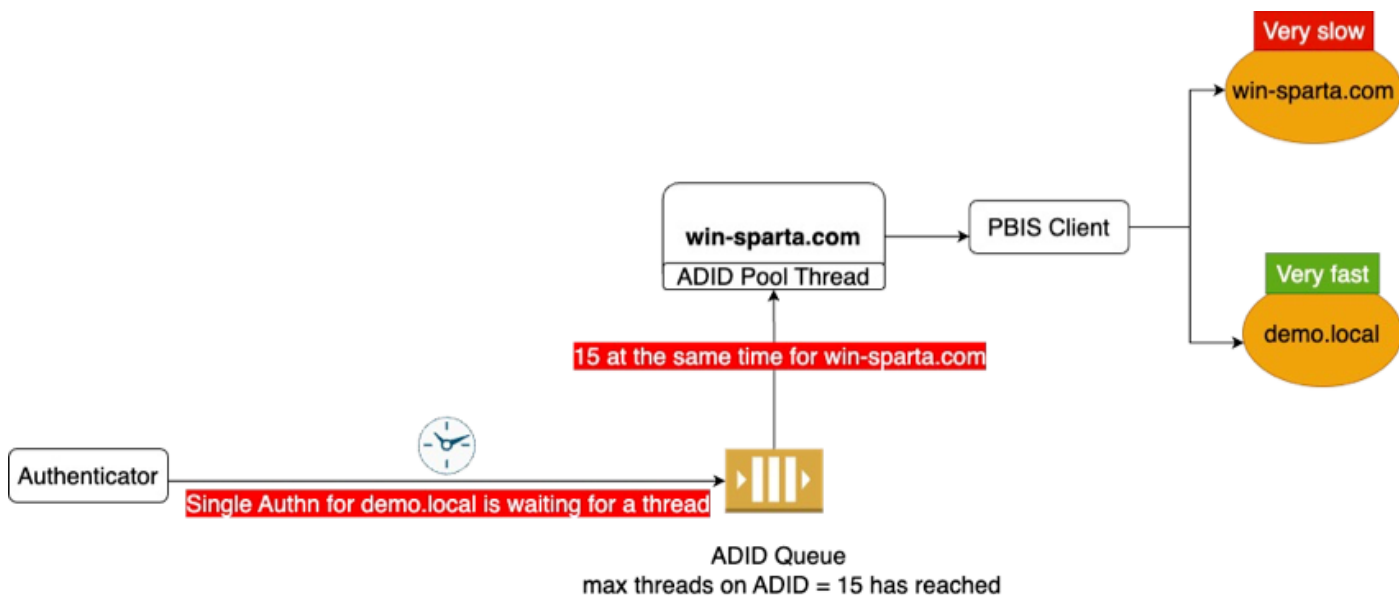
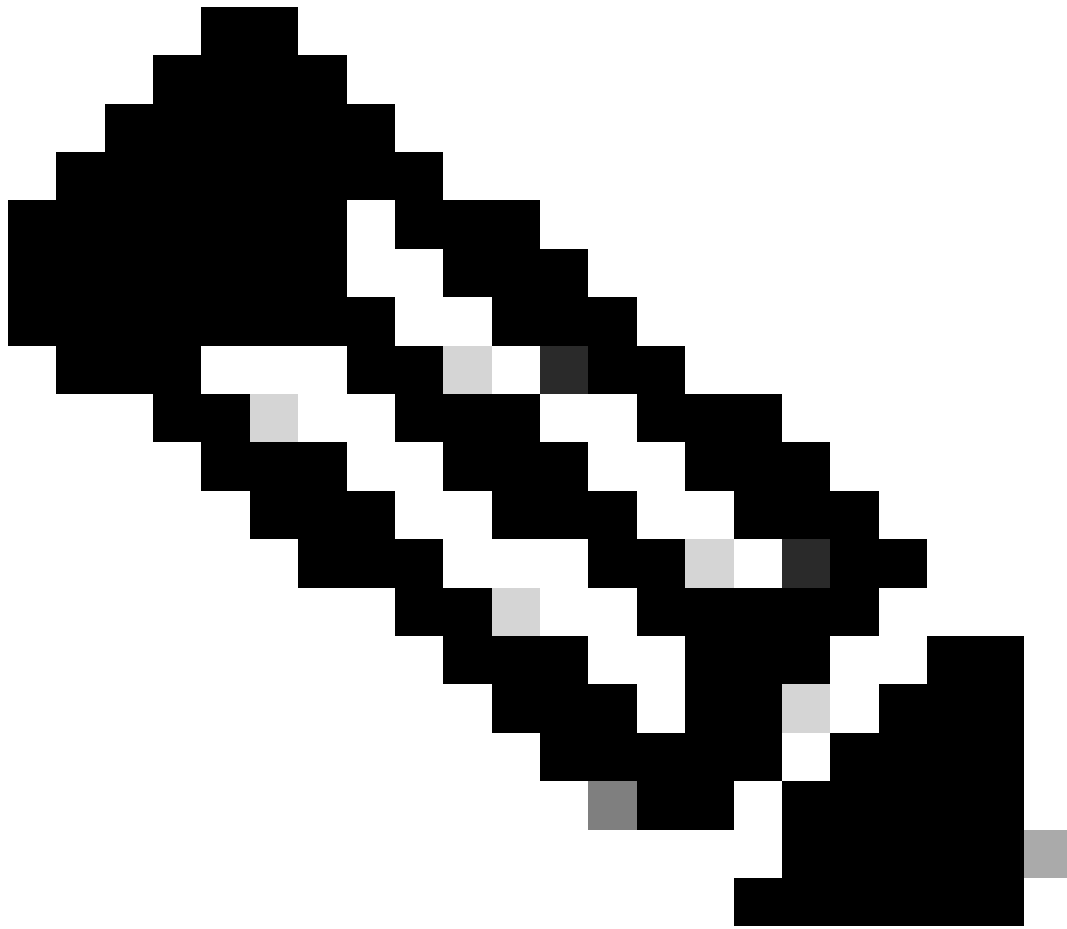


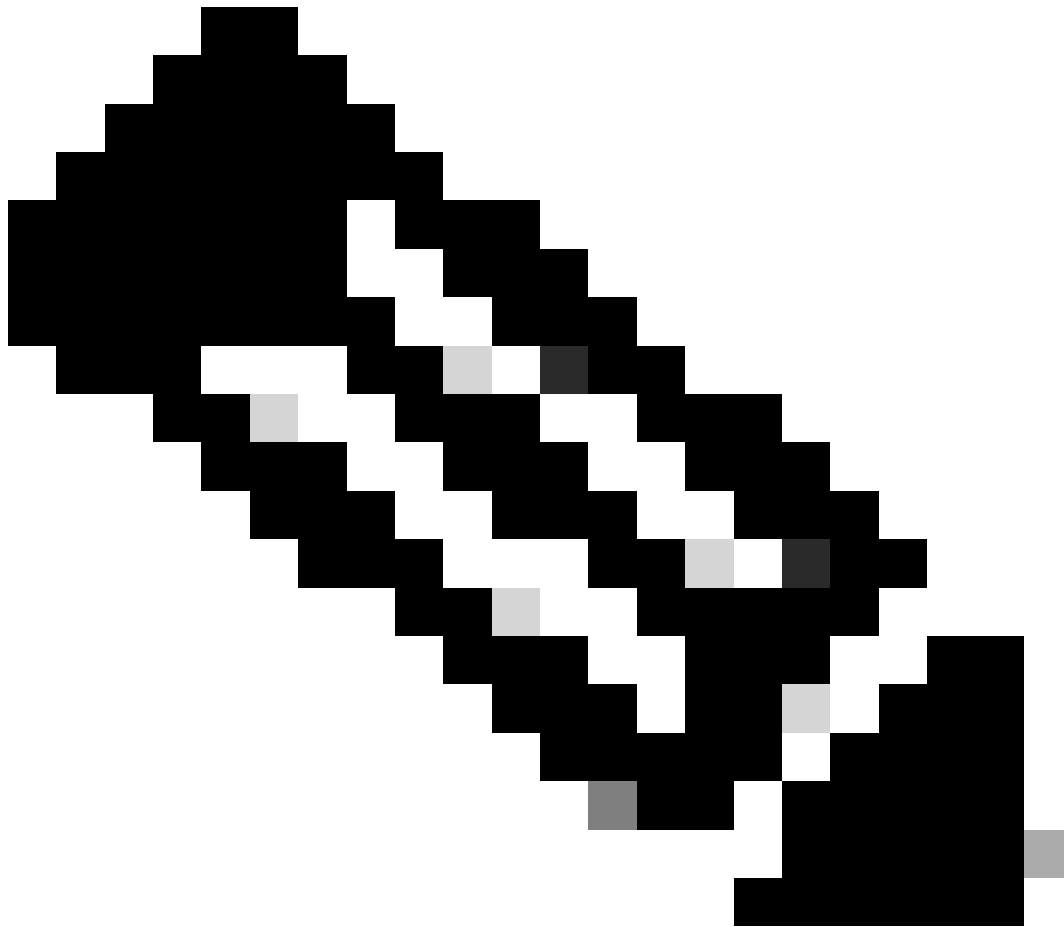
图 3：有问题的流



注意：此处，所有15个线程同时被win-sparta.com占用，没有线程用于demo.local

解决方案

- 默认行为是所有AD加入点的公共线程池
- 但是，管理员可以对每个加入点进行分段以拥有自己的资源。



注意：应用AD优先级时，默认每个线程池为10个线程。

请参阅图4:按需预留节点流程图



图 4：解决方案流程

逐步配置

步骤1:创建2个单独的AD加入点。例如：demo.local和win-sparta.com

步骤2:创建AD加入点后创建加入点优先级。

请参阅图5:

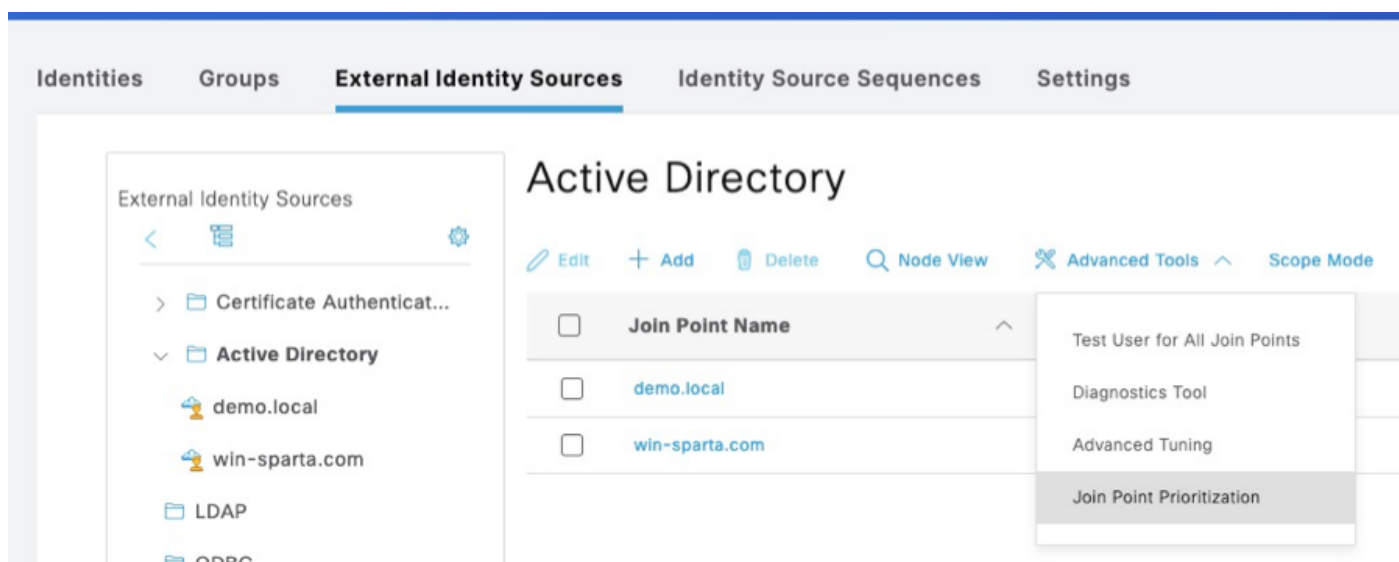


图 5：加入点优先级

步骤3:在Join Point Prioritization下，选择您想要保留专用AD资源的PSN。单击 Edit。

请参阅图6:

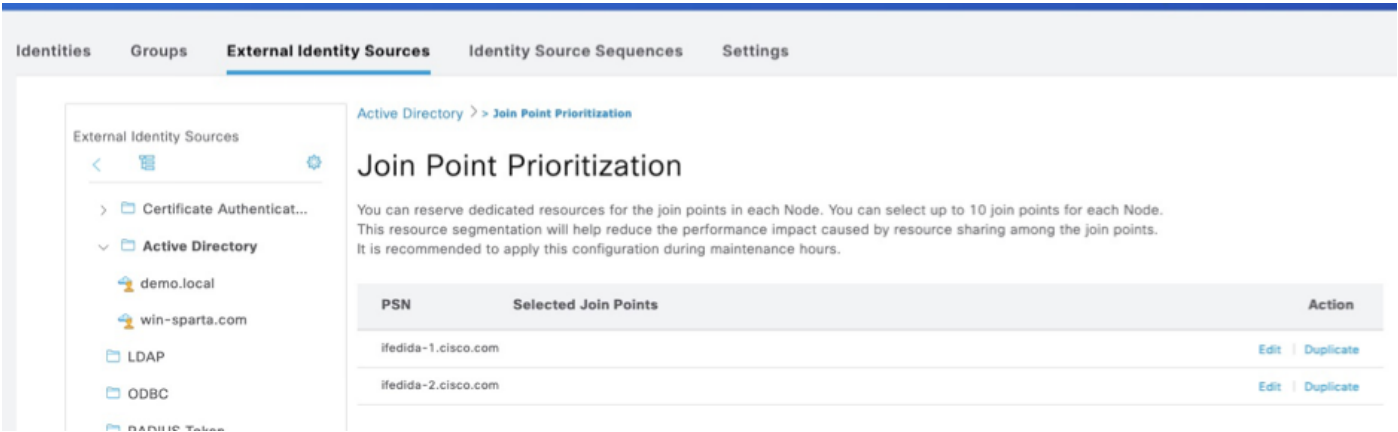


图 6：编辑PSN

第4步：选择首选PSN的首选连接点。

请参阅图7:

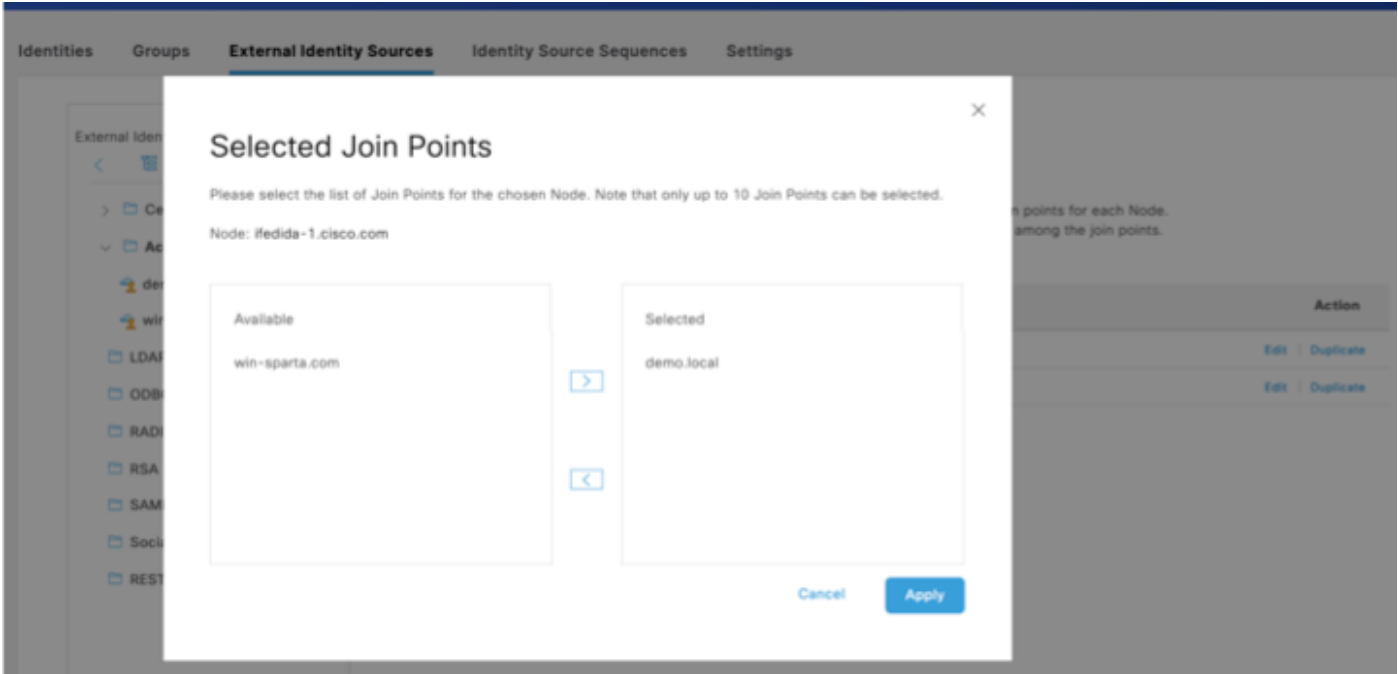


图 7：选定的加入点



注意：未包括在优先级中的任何加入点都使用公共线程池，该池最多限制为15个线程。

第5步：最终确定优先级

请参阅图8:

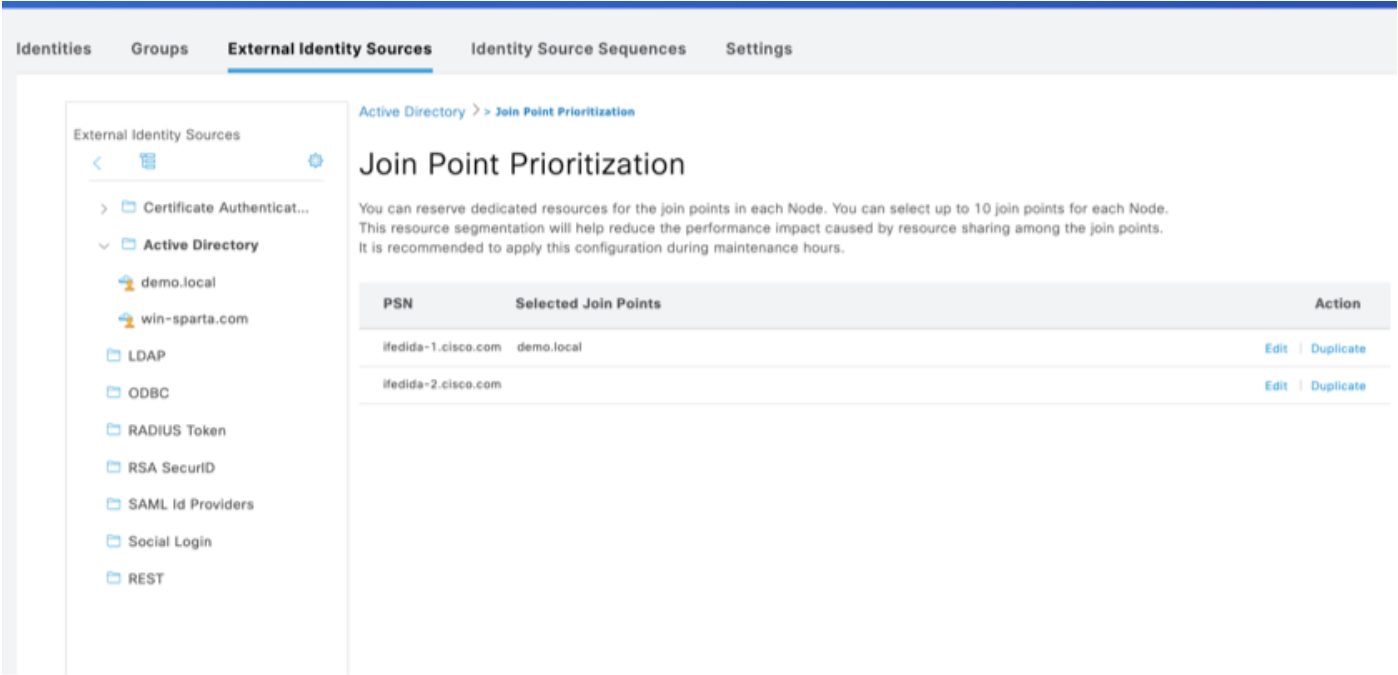
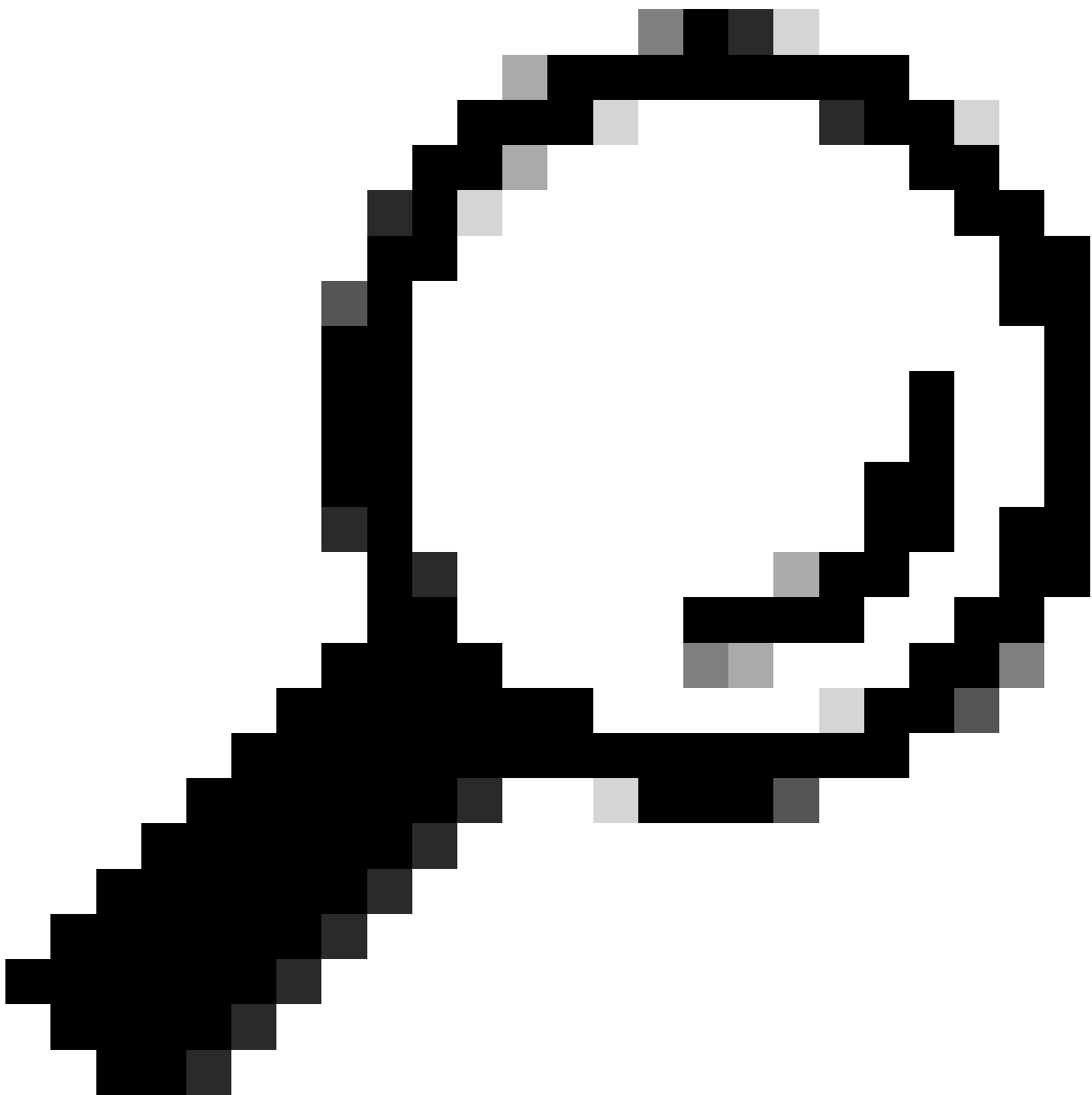


图 8：优先级配置

其他详细信息



提示：如果要相同的设置复制到其他PSN，可以使用Duplicate选项。选择所需的PSN，然后选择要与原始优先级一起复制的加入点。

请参阅图9:配置提示：

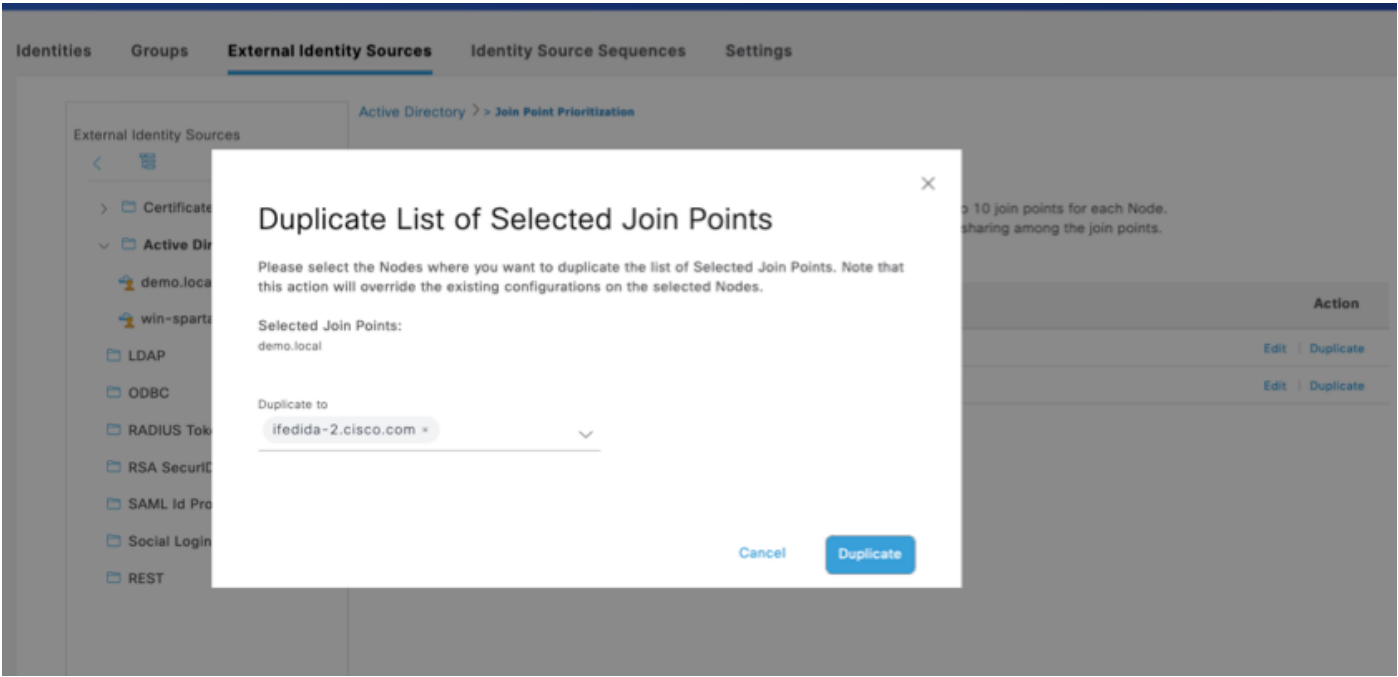


图 9：重复优先级配置

步骤6:复制后的最终列表

请参阅图10:

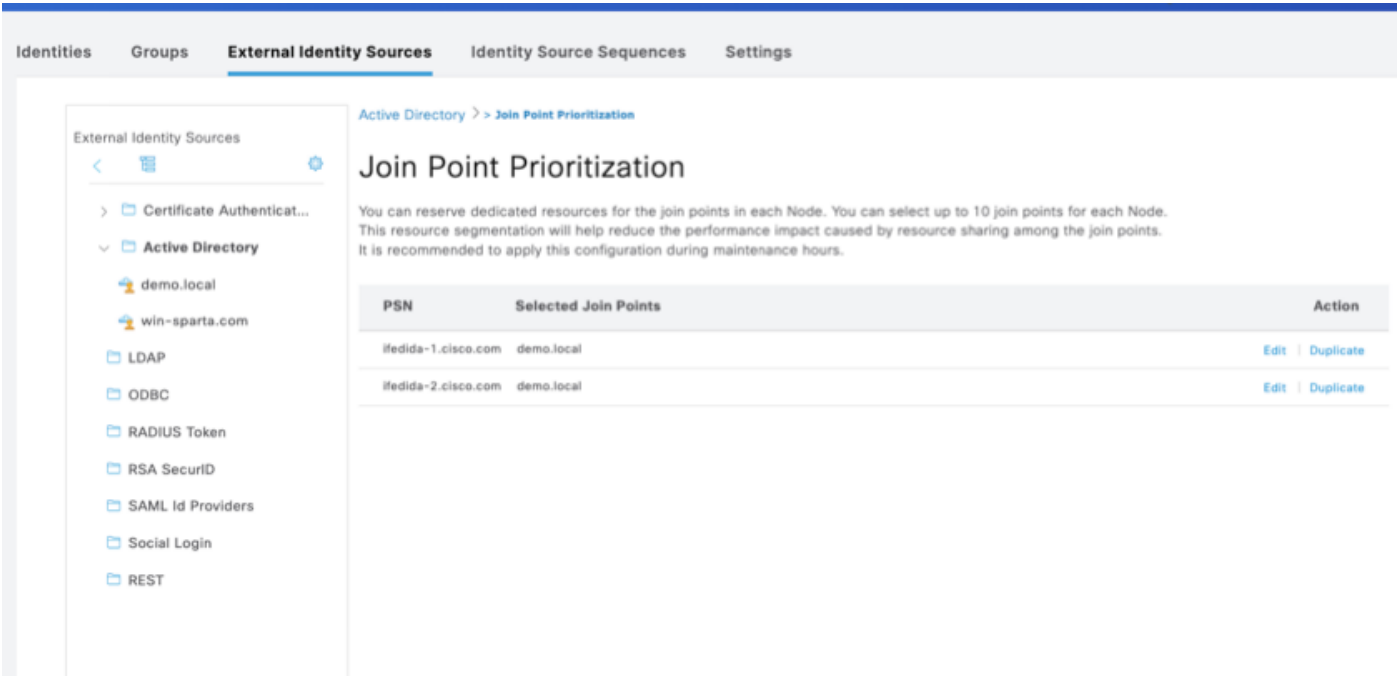


图 10：确定优先级后的最终列表

故障排除

确认

检验配置更改。导航至：运营>报告>审核>更改配置审核

请参阅图11:

Reports

Export Summary

My Reports

Reports

Audit

Adaptive Network Control Audit NLS

Administrator Logins

Change Configuration Audit

Cisco Support Diagnostics Audit

Data Purging Audit

Endpoints Purge Activities

Internal Administrator Summary

IPSec Audit Logging

Change Configuration Audit

From 2024-09-04 00:00:00.0 To 2024-09-04 15:42:38.0

Reports exported in last 7 days: 0

Add to My Reports

Export

Filter

Logged At	Administrator	Server	Interface	Object Type	Object Name	Event
Today	Administrator	Server		Object Type	Object Name	
2024-09-04 15:41:20.5...	admin	ifedida-2	GUI	AD Join point prioritization settings	AD Join point prioritization	Changed configuration
2024-09-04 15:41:20.4...	admin	ifedida-2	GUI	AD Join point prioritization settings	AD Join point prioritization	Changed configuration

图 11：配置审核报告

日志记录

- 启用运行时AAA日志的调试级别。
 - 分析prrt-server.log
- 请参阅图12:

☐	runtime-AAA	DEBUG	AAA runtime messages (prrt)	prrt-server.log
-----------------------	-------------	-------	-----------------------------	-----------------

图 12：调试日志配置

日志片段

prrt-server.log [DEBUG]：默认日志：

EventHandler，2024-08-23 07:16:48,135,DEBUG，0x7fecd2ccc700，分配的默认线程池：添加至IDP:win-sparta.com_wxETIH16Pk_106

prrt-server.log [INFO]：设置专用资源时执行以下操作:

- ActiveDirectoryIDStore，2024-09-08 16:52:01,048,INFO，0x7f2452ccf700，分配的线程池：ADThreadPool0到IDP :win-sparta.com_wxETIH16Pk_106
- ActiveDirectoryIDStore，2024-09-08 16:57:11,258,INFO，0x7f2452ccf700，分配的线程池：ADThreadPool1到IDP:demo.local_6EcNs6UzwX_89

prrt-server.log [信息]:

- 在设置专用资源之前：
 - EventHandler，2024-09-02 08:45:54,673,INFO，0x7fafb793c700，将事件传递到下一个线程池名称=ADIDStore，队列大小=1,EventDispatcher.cpp:757
- 在我们设置专用资源后：

- EventHandler , 2024-09-02 08:45:54,673,INFO , 0x7f4867ff9700 , 将事件传递到下一个线程池名称=ADThreadPool0 , 队列大小=1,EventDispatcher.cpp:841

跟踪"ADThreadPool0"的线程池使用情况 :

1.0x7f57792f7700 , 将事件传递到下一个线程池名称= ADThreadPool0 (很少回滚
StackID:0x7f57a4f761c0)

2. 0x7f57732c7700 , 堆叠 : 0x7f57a4f761c0调用ActiveDirectoryIDStore:方法
MethodCaller<ActiveDirectoryIDStore , PlainAuthenticateAndQueryEvent>

3. 0x7f57732c7700,cntx=0000210117,sesn=ifedida-
1/515863662/5273,CPMSessionID=C0A31430000000800018958,user=abcd , CallingStationID=[CAD]
956:已调用CAD_PAPAuthenticate(abcd)

4. 0x7f57732c7700,cntx=0000210117,sesn=ifedida-
1/515863662/5273,CPMSessionID=C0A31430000000800018958,user=abcd,CallingStationID=[CAD]
1026:CAD_PAPAuthenticate(abcd)成功

5. 0x7f57732c7700 , 将事件传递到下一个线程池名称=Main

常见问题

问题 : ISE可以支持多少个AD加入点 ?

回答 : 您可以在单个ISE部署上配置最多50个Active Directory加入点。

问题 : 如果我有多个AD加入点 , 是否仍可以使用按需优先排序 ?

回答 : Yes

问题 : 单个域没有优先级的默认线程大小是多少 ?

回答 : 15个线程

问题 : 如果配置优先级 , 如何进行计算 ? 考虑一下 , 未为优先级配置带domain1.com的3个加入点场景 — domain1.com、domain2.com和domain3.com , 为优先级配置了domain2.com和domain3.com。

回答 : 如果未将domain1配置为优先排序 , 则domain1.com会同时使用常用的15个线程。但是 , 由于domain2.com和domain3.com配置了优先级 , 因此它们默认使用10个线程 , 而不遵循/利用公用15个线程池。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。